

Ref. 1

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11032088 A**

(43) Date of publication of application: 02 . 02 . 99

(51) Int. Cl.

H04L 12/66
G06F 13/00
G06F 13/00
H04L 12/46
H04L 12/28
H04L 12/24
H04L 12/26

(21) Application number: **09186850**

(22) Date of filing: **11 . 07 . 97**

(71) Applicant: **HITACHI LTD**

(72) Inventor: **KONDO TAKESHI**
NAKADA YUKIO
AKAOSUGI TAKASHI

(54) **NETWORK SYSTEM**

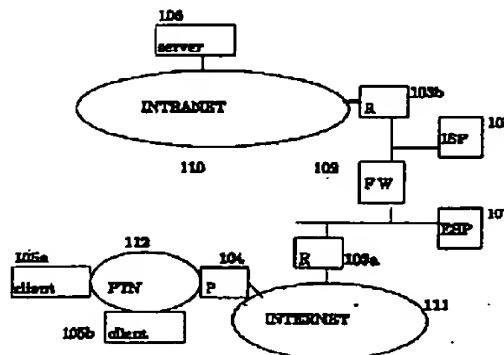
extendability is high.

(57) Abstract:

COPYRIGHT: (C)1999,JPO

PROBLEM TO BE SOLVED: To execute safe communication via a fire wall(FW) without altering an application program by performing communication with a second data communication means and transferring the data of a specified application program without mutually constructing a data transfer path and changing a specified program on a computer.

SOLUTION: An FW 102 is provided with a socket-processing part and a TCP/IP processing part, and a main processing part is a circuit gateway type operated as the application program(AP) of the FW 102, transmits and receives the ID of a connection destination and a transmitter and relays the data from the transmitter confirmed by an authentication processing part. An ESP 101 is composed of an ISP protocol processing part for performing the communication with an ISP 100 and a client protocol processing part for performing the communication with a client, and in the case of coping with the various APs, only setting information needs to be changed by using a text editor, so that development cost is reduced and



THIS PAGE BLANK (USPTO)

【特許請求の範囲】

【請求項1】 相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと接続される第1のデータ通信手段と、前記汎用アクセスチェック装置で保護されていないネットワークに接続される第2のデータ通信手段と、前記第1と第2のデータ通信手段の相互間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記第2のデータ通信手段と通信を行って前記特定アプリケーションプログラムのデータを転送する手段と、前記第1の通信手段と第2の通信手段との間のデータ転送パスを用いて前記特定アプリケーションプログラムのデータを中継するデータ中継手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムのデータ中継手段を制御する手段とを備えたことを特徴とするネットワークシステム。

【請求項2】 クライアント計算機と汎用アクセスチェック装置との間の通信路が暗号化されており、前記第1のデータ通信手段が特定アプリケーションプログラムのデータ内容の判定機能を持つことを特徴とする請求項1記載のネットワークシステム。

【請求項3】 前記第1のデータ通信手段と第2のデータ通信手段とが独立した専用装置として構成されることを特徴とする請求項1または2記載のネットワークシステム。

【請求項4】 前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを用いて前記データ中継手段を制御する手段への初期化情報を配布する機能を備えたことを特徴とする請求項1、2または3記載のネットワークシステム。

【請求項5】 クライアント計算機と汎用アクセスチェック装置との間で認証データを中継する認証データ中継装置を備え、前記汎用アクセスチェック装置に認証機能を備え、認証が終了したらその認証結果に基づいて前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを用いてクライアント計算機のデータの中継を実行することを特徴とする請求項1ないし4のうちのいずれか1記載のネットワークシステム。

【請求項6】 前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを暗号化する機能を備えたことを特徴とする請求項1ないし5のうちのいずれか1記載のネットワークシステム。

【請求項7】 前記第1のデータ通信手段または第2の

データ通信手段とクライアント計算機との間のデータを暗号化する機能を備えたことを特徴とする請求項1ないし6のうちのいずれか1記載のネットワークシステム。

【請求項8】 前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを用いて、第1のデータ通信手段と第2のデータ通信手段との間でアプリケーションプログラムデータの転送制御用の情報を送受信することを特徴とする請求項1ないし7のうちのいずれか1記載のネットワークシステム。

【請求項9】 前記第1のデータ通信手段と第2のデータ通信手段との間の1つのデータ転送パスを用いて、複数の特定アプリケーションプログラムデータを中継することを特徴とする請求項1ないし8のうちのいずれか1記載のネットワークシステム。

【請求項10】 前記第1のデータ通信手段と第2のデータ通信手段との相互間で、相互を認証する機能を備えたことを特徴とする請求項1ないし9のうちのいずれか1記載のネットワークシステム。

【請求項11】 前記第1のデータ通信手段と第2のデータ通信手段との間を直接伝送路で接続し、前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを、前記伝送路を用いて構築したことを特徴とする請求項1ないし10のうちのいずれか1記載のネットワークシステム。

【請求項12】 前記クライアント計算機は、汎用アクセスチェック装置を介してサーバ計算機と接続するか、第2のデータ通信手段を介して接続するかを振り分ける機能を有することを特徴とする請求項1ないし11のうちのいずれか1記載のネットワークシステム。

【請求項13】 前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを、第2のデータ通信手段が複数の第1のデータ通信手段との間に確立させることを特徴とする請求項1ないし12のうちのいずれか1記載のネットワークシステム。

【請求項14】 前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを、第1のデータ通信手段が複数の第2のデータ通信手段との間に確立させることを特徴とする請求項1ないし12のうちのいずれか1記載のネットワークシステム。

【請求項15】 前記汎用アクセスチェック装置により保護されているネットワークにおけるセキュリティポリシー情報を、前記第2のデータ通信手段に前記第1のデータ通信手段と第2のデータ通信手段との間のデータ転送パスを用いて反映させる機能を備えたことを特徴とする請求項1ないし14のうちのいずれか1記載のネットワークシステム。

【請求項16】 相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構

成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと前記汎用アクセスチェック装置で保護されていないネットワークとの両方に接続される特定アプリケーションプログラム用アクセスチェック装置と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記特定アプリケーションプログラム用アクセスチェック装置と通信を行い、前記特定アプリケーションプログラムのデータをクライアント用アプリケーションプログラムを変更することなく前記アプリケーションプログラム用アクセスチェック装置に転送する手段と、前記特定アプリケーションプログラム用アクセスチェック装置で特定アプリケーションプログラムのデータを中継する中継手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムの中継手段を制御する手段とを備えたことを特徴とするネットワークシステム。

【請求項17】 相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記アクセスチェック装置は、ネットワークと直接接続されない汎用的なアクセスチェックプログラムと、保護されたネットワークを用いて通信を行う第1のプログラムと、保護されていないネットワークを用いて通信を行う第2のプログラムと、前記3つのプログラム相互間の通信手段と、特定アプリケーションプログラムのデータ内容に応じて汎用的なアクセスチェックプログラムを介したデータ中継処理を制御する手段と、前記クライアント計算機上の特定アプリケーションプログラムを変更することなく前記アクセスチェック装置との通信を行う手段とを備えたことを特徴とするネットワークシステム。

【請求項18】 相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のアプリケーションプログラムとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されているネットワークに接続される第1の装置と前記と異なる汎用アクセスチェック装置で保護されたネットワークに接続する第2の装置とを設け、前記複数の汎用アクセスチェック装置を介して前記第1と第2の装置との間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定アプリ

ケーションプログラムを変更することなく、前記第2の装置と通信を行い、前記特定アプリケーションプログラムのデータを前記第2の装置に転送する手段と、第1の装置と第2の装置との間のデータ転送パスを用いて特定アプリケーションプログラムのデータを配送する手段と、特定アプリケーションプログラムのデータ内容に基づいて前記特定アプリケーションプログラムのデータ転送手段を起動する手段とを備えたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ネットワークシステムに係り、特に、イントラネットやインターネット等のネットワークを利用し、すでに使用している多様なアプリケーションプログラム（以下、APという）を改造することなく使用して、安全な通信を行うことのできるセキュリティ性の高いネットワークシステムに関する。

【0002】

【従来の技術】 ネットワークへの不正なアクセスを防止することによりネットワークシステムの安全性の向上を図ることのできる従来技術として、FW(Fire Wall)構築技術が知られている。このFW構築技術には、アプリケーションゲートウェイ（以下、APGWという）、サーキットゲートウェイ（以下、SCGWという）、パケットフィルタ等が知られてる。

【0003】 パケットフィルタに関する従来技術として、例えば、特開平5-327717号公報に記載された技術が知られている。この従来技術は、端末アドレスとポート番号との組でパケットをフィルタするというものである。また、SCGWに関する従来技術として、Internet-Draftsにおける“SOCK Protocol Version 5”に記載された技術が知られている。

【0004】 その他、前述したようなネットワークへの不正なアクセスの防止だけでなく、ネットワーク上のデータの盗聴や改竄を防止するため、通信路を暗号化するVPNを構築可能とするFWも知られており、この実現の技術としてトンネル技術によるVPNを構築することも知られている。

【0005】

【発明が解決しようとする課題】 前述したSCGW方式のFWは、通信ポートが固定でないAPを、既存のAPを改造することなく実現することができないという問題点を有し、また、APGWと併用したパケットフィルタFWは、通信ポートが固定でないAPをサポートすることができるが、そのためには、AP毎に対応したAPGWを用いなければならない、その開発コストが高く、また、性能的に劣っているという問題点を有している。

【0006】 本発明の目的は、前述した従来技術の問題点を解決し、SCGW方式のFWを用いたネットワークシステムにおいて、通信ポートが固定でないAPを、既

存のAPを無改造なまま使用してFWが備えるアクセスチェック機能を実現することを可能とし、開発コストが低く性能的に劣らないセキュリティ性能を持ったネットワークシステムを提供することにある。

【0007】また、本発明の目的は、前述の動的ポートを使用する多種多様な個別APのVPN構築を容易に実現することのできるネットワークシステムを提供することにある。

【0008】

【課題を解決するための手段】本発明によれば前記目的は、APインタフェースに変更を加えずに前述した目的を達成するために、FWにある特定のアクセス可能なポートを設け、また、そのポートを用いて許可されたAPのデータを転送する次の2つの手段を設けることにより達成される。すなわち、第1の手段は、FWを挟み込む形で前記ポートを用いた通信路を確立し、この通信路を用いてAPデータを中継する中継手段であり、第2の手段は、APが動的ポートを使用するため通知する動的ポート通知を認識し、これを通知したAPのアクセス権限をチェックし、許されたAPならば、以後の動的ポートを用いたAPデータを前記中継手段を用いた通信に切り替える手段である。なお、前記中継手段に、APデータの暗号化を行う手段を設けるとよい。

【0009】本発明は、前述の構成を備えることにより、中継手段がFWのアクセス可能ポートを用いてAPデータを転送するため、動的ポートを使用するAPを無改造で使うことができ、また、許可されたAPデータのみを中継手段を使用した通信に切り替えるようにすることにより、そのアクセスチェックも行うことが可能となる。

【0010】また、前述の中継手段の通信路を暗号化することによりFWを介したVPNを動的ポートを使用するAPにおいて実現することができる。

【0011】本発明によれば前記目的は、具体的には、相互接続された計算機ネットワークに接続されたクライアント計算機と、前記計算機ネットワークに汎用アクセスチェック装置を介して接続され保護されたネットワークに接続されたサーバ計算機とから構成され、前記サーバ計算機と前記クライアント計算機上のAPとの間でデータ通信を行う計算機ネットワークシステムにおいて、前記汎用アクセスチェック装置により保護されたネットワークと接続される第1のデータ通信手段と、前記汎用アクセスチェック装置で保護されていないネットワークに接続される第2のデータ通信手段と、前記第1と第2のデータ通信手段の相互間にデータ転送パスを構築する手段と、前記クライアント計算機上の特定APを変更することなく前記第2のデータ通信手段と通信を行って前記特定APのデータを転送する手段と、前記第1の通信手段と第2の通信手段との間のデータ転送パスを用いて前記特定APのデータを中継するデータ中継手段と、特

定APのデータ内容に基づいて前記特定APのデータ中継手段を制御する手段とを備えることにより達成される。

【0012】前述した本発明の目的を達成するための構成の種々の変形例は、発明の実施形態の説明において詳細に説明する。

【0013】

【発明の実施の形態】以下、本発明によるネットワークシステムの実施形態を図面により詳細に説明する。

【0014】図1は本発明の第1の実施形態によるネットワークシステムの構成例を示すブロック図であり、FWを介してインターネットとイントラネットとを接続して構成されたネットワークシステムである。図1において、100は内部セキュリティ代行サーバ(Intra Security Proxy: 以下、ISPという)、101は外部セキュリティ代行サーバ(Extra Security Proxy: 以下、ESPという)、102はFW、103はルータ(以下、Rという)、104はインターネットプロバイダ(以下、Pという)、105はクライアント計算機、106はサーバ計算機、110はイントラネット、111はインターネット、112は公衆電話網(Public Telephone Network: 以下、PTNという)である。

【0015】図1に示すように構成されるネットワークシステムにおいて、クライアント計算機105a、105b(両者を区別する必要のない場合、単に105と記す)は、PTN112に接続されたP104、インターネット111、R103a、FW102、R103bを介してイントラネット110内のサーバ計算機106にアクセスする。クライアント計算機105からサーバ計算機106へのアクセスにおいて、FW102は、正当なアクセスのみを中継する。また、R103a、103b(両者を区別する必要のない場合、単に103と記す)は、ネットワーク間を接続しデータパケットの振り分けを行う。図示ネットワークシステムは、イントラネット110へのアクセスに対する保護を強固なものとするため、各ネットワーク相互間をFW102とR103とを介して接続する。

【0016】FW102とインターネット側のR103aとが接続されたセグメントには、ESP101が接続されている。また、FW102の内側のセグメントには、ISP100が接続されている。ISP100とESP101とは、両者が協力してFW102の持つアクセスチェック機能を補完する。FW102、クライアント105、サーバ106、ESP101、ISP100は、共にCPUとメモリとからなるよく知られた計算機システムにより構成されている。

【0017】図2はクライアント計算機105のソフトウェア構造を説明する図であり、以下、これについて説明する。

【0018】図2において、200はクライアント用A

Pであり、種々の処理を行う通信プログラムである。クライアント用APは、具体的には、ファイル転送、テルネット、ネットワークチャット等、あるいは、その他の業務用処理を行うプログラムであり、OS 203上で動作する。OS 203は、通信プロトコルを制御してインターネット111上でのデータ送受信処理を担当するTCP/IP処理206とPTN112を介したP104とのデータ送受信処理を担当するPPP処理207とを含む。

【0019】また、クライアント計算機105は、クライアント用AP200とTCP/IP処理203とのインタフェースを処理するソケット処理202を含む。従来の処理では、クライアント用AP200がソケット処理202を直接呼び出すが、本発明では、ソケット処理202とクライアント用AP200との間にソケットフック処理201をミドルウェアとして設けている。また、本発明の第1の実施形態では、補助アプリケーションとして目的のP104との間でPPP処理207を起動させるプロバイダアクセス処理205を持ち、また、PTN112上の伝送制御を行うモデムドライバ204を含む。

【0020】ソケットフック処理201は、クライアント用AP200とのインタフェースとしてソケット処理202と全く同一のインタフェースを提供し、かつ、ソケット処理202とのインタフェースを利用してクライアント用AP200にソケットインタフェースを提供する。また、ソケットフック処理201は、認証・暗号・アクセス先制御機能を持つ。このソケットフック処理201により、クライアント用APは、無改造でFW102を含むネットワークシステムに適応することができる。

【0021】図3はFW102のソフトウェア構成を説明する図であり、以下、これについて説明する。図3において、300はFWメイン処理であり、FWメイン処理300は、中継処理301、認証処理302、ネゴシエーション処理303から構成される。また、FW102は、クライアント計算機105と同様にソケット処理202とTCP/IP処理203とを持つ。

【0022】FWメイン処理300は、FW102のAPとして動作する。このFW102は、サーキットゲートウェイ型であり、ネゴシエーション処理303で接続先や送信者のIDを送受し、認証処理302により確認した送信者からのデータを中継処理301がソケットレベルで中継する。この中継処理301は、データを暗号化して送るといった機能を有していない。

【0023】図4はESP101のソフトウェア構成を説明する図であり、以下、これについて説明する。図4において、403はESPメイン処理であり、ESPメイン処理403は、ISP100との通信を行うISPプロトコル処理400、クライアントとの通信を行うク

ライアントプロトコル処理401、データの中継を行う中継処理402から構成される。また、FW102と同様にソケット処理202とTCP/IP処理203とを持つ。

【0024】図5はISP100のソフトウェア構成を説明する図であり、以下、これについて説明する。図5において、500はISPメイン処理であり、ISPメイン処理500は、ESPとの通信を行うESPプロトコル処理502、APデータ解析制御処理501、中継処理503から構成される。また、FW102やESP101と同様にソケット処理202とTCP/IP処理203とを持つ。また、506はISP100のOSであり外部I/O装置との入出力を制御する。このOS506は、設定情報505を変更するテキストエディタ504を備える。設定情報には、後に説明する各AP毎の動的アドレス通知を判定する条件がテキストとして記述されている。APデータ解析制御処理501は、前述の条件に基づいて動的アドレス通知の判定処理を実行する。

【0025】前述したように、ISP100は、多様なAPへ対応する場合、テキストエディタ504を使用して設定情報を変更すればよいので、APGW方式のFWを追加するより開発コストが少なくすみ、かつ、拡張性もよいという効果を得ることができる。

【0026】図6は本発明の第1の実施形態による図1に示すネットワークシステムにおけるESPとISPとの間のプロトコルを説明するシーケンス図であり、図6を参照して、各装置における処理を詳細に説明する。

【0027】(1) まず、ISP100とESP101との間でFW102を介した通信を行い、ISP100とESP101との初期化を行い、論理的セッションを開設する。この後、クライアント105のAP200は、サーバ106とのコネクションを確立するためのconnect要求を発行する(ステップ600、601)。

【0028】(2) 次に、クライアント用AP200からのコネクト要求を受けたソケットフック処理201は、コネクション確立先をサーバ106からESP101に換えてコネクションを確立する(ステップ602)。

【0029】(3) クライアント105のソケットフック処理201からのコネクションを受諾したESP101は、FW102の持つ認証機能を利用するため、FW102に対してコネクションを確立し、次に、クライアント認証を行うために必要な情報の中継処理を行う。このようにして、クライアント105の認証がESP101を介してFW102で行われる(ステップ603、605)。

【0030】このように、本発明の実施形態によるESP-ISP間のプロトコルは、FW102の認証機能を利用しているため、ESP101やISP100に認証

のためのデータベースを持つ必要がなく、認証情報を設定する必要がなく管理がしやすいという利点がある。

【0031】(4) ステップ605の認証シーケンスの途中において、FW102は、クライアント105を確認すると、サーバ106とのコネクションを確立する(ステップ604)。

【0032】(5) そして、ステップ605の最後にFW102は、中継路が確立したことをクライアント105へ通知する。このFW102の中継経路確立通知を受けたESP101は、すぐにクライアント105への中継を行わず、以下に説明する一連の処理が終了するまで前記通知を保留する。次に、ESP101は、FW102とのコネクションを解放することにより、FW102の中継路を解放する(ステップ606)。

【0033】(6) 次に、ESP101は、一時的な暗号鍵を生成してクライアント105との間でこの暗号鍵を交換する(ステップ607)。

【0034】このように、コネクション単位の暗号鍵を使用することにより暗号鍵の推定がしにくくなりセキュリティを高めることができる。また、FW102に暗号化機能が無くても、ESP101が暗号化機能をFW102の変更をせずに実現することができるという利点を持つ。

【0035】(7) 次に、ESP101は、ISP100を介したサーバ106とのコネクション要求を、ステップ600で先に確立したセッションを通じて送る。これを受けた、ISP100は、サーバ106とのコネクションを確立し、その応答をESP101に返す(ステップ608~610)。

【0036】(8) これを受けたESP101は、保留しておいた中継路確立応答をクライアント105側に返す。このESP101からの中継路確立応答を受けたソケットフック処理201は、AP200に対して正常リターンすることにより、サーバ106とのコネクションが確立したことをAP200へ通知する(ステップ611、612)。

【0037】前述した処理により、クライアント105とサーバ106との仮想的なコネクションが、ISP100、FW102、ESP101の各コネクションを中継した形で実現できる。

【0038】次に、前述の処理により確立したコネクションを通じてデータが送られる際のシーケンスについて説明する。

【0039】(9) クライアント用AP200は、データを送るときソケットフック処理201に対して送信データとコネクションとを指定したsend要求を発行する。これを受けたソケットフック処理201は、ESP101に対してAP200からのデータを送信する(ステップ613、614)。

【0040】(10) クライアント105からのデータを

受信したESP101は、データをカプセル化してISP100へ渡す。このカプセル化されたデータを受けたISP100は、そのデータの内容をチェックし、クライアントによる通信アドレスの通知であるか否かを判定する(ステップ615、616)。

【0041】(11) ステップ616のチェックで条件に合致しない場合、ISP100は、カプセル化されたデータを元のデータに戻し、ステップ609で確立したコネクションを用いてデータをサーバ106に渡す。ステップ616のチェックで条件が合致した場合、すなわち、クライアントによる通信アドレスの通知であった場合、ISP100は、ESP101にクライアント105とのコネクション確立要求を送る(ステップ617、618)。

【0042】(12) これを受けたESP101は、クライアント105とのコネクションを確立する。このときコネクションの受け入れ待ちとなるクライアント用AP200は、accept要求をソケットフック処理201に対して要求しておく。そして、ソケットフック処理でステップ619によるESP101とのコネクションが確立したら、ソケットフック処理201は、そのことをAP200にリターンにより通知する(ステップ619~621)。

【0043】(13) クライアント105とのコネクションを確立したESP101は、その結果をISP100に通知する。このコネクション確立通知を受けたISP100は、ステップ616で保留した中継APデータ中のクライアントの通信アドレスをISP100自身の通信アドレスに変えてサーバ106に送る(ステップ622、623)。

【0044】(14) ISP100から通信アドレスを受けたサーバ106は、ISP100の通信アドレス宛にコネクションを張り、これにより確立したコネクションを用いてデータを転送する(ステップ624、625)。

【0045】(15) これを受けたISP100は、データをESP101へ中継する。このサーバ106からのデータを受けたESP101は、クライアント105にステップ619で確立したコネクションを用いてそのデータの中継する。クライアント用AP200は、データを受け取るためrecv要求を発行しておき、その応答としてデータを受け取る(ステップ626~629)。

【0046】前述したシーケンスを処理するISP100とESP101、及び、クライアント105のソケットフック処理201により、SCGWタイプのFW102を介して接続されるクライアント105とサーバ106とにおいて、クライアント用AP200が、サーバ106に対して動的に割り当てられたクライアント用AP200の通信アドレスを通知し、これを受けたサーバ106から通知されたクライアント通信アドレス宛にデー

タを送信する処理を行うアプリケーションプログラムのアクセスチェックを当該アプリケーションを改造することなく実現することができる。

【0047】図7は図6により説明したISP100とESP101との間の通信プロトコルメッセージのフォーマットを説明する図である。

【0048】図7において、700は共通フォーマットであり、この共通フォーマット700は、コマンドフィールド701、コネクションIDフィールド702、コマンド個別フィールド703の3つのフィールドから構成される。そして、コマンド個別フィールド703のみ可変長であり、その他のフィールドは固定長であり、コマンドフィールド701内の値によって各種メッセージが判別できる。

【0049】710はコマンドフィールド701内の値とその名称を示した表である。各コマンドには、次の5種類がある。すなわち、ステップ608に対応するinside-connect.req、ステップ610に対応するinside-connect.rsp、ステップ615と626に対応するdata-transfer.req、ステップ618に対応するoutside-connect.req、ステップ622に対応するoutside-connect.rspの5つである。

【0050】また、720は前述の各コマンドにおけるコネクションIDフィールド702の内容を示した表である。この表720におけるoutside-connection IDは、ESP101がシーケンスのステップ602で確立するクライアント105とのコネクションを識別する番号である。また、inside-connection IDは、ISP100がシーケンスのステップ624で確立するサーバ106とのコネクションを識別する番号である。

【0051】730は前述の各コマンドにおけるコマンド個別フィールド703の内容を示した表である。この表730におけるinside-connect.reqのserver addressは、サーバ106の通信アドレスである。また、inside-connect.rspの結果codeは、ステップ609の結果を示す値であり、data-transfer.reqのApplication dataは、サーバ106とクライアント105との間で転送される通信データである。さらに、outside-connect.reqのclient addressは、ステップ616のチェックで該当するデータをサーバ106へ送ったクライアント105の通信アドレスであり、outside-connect.rspの結果codeは、ステップ619で確立されるESP101とクライアント105とのコネクションの結果である。また、new outside-connecti

on IDは、ステップ619で確立されるESP101とクライアント105との間のコネクションを識別する番号である。

【0052】図8はISP100とESP101との間の初期化用セッション確立の処理を説明するシーケンス図であり、次に、前述したFW102を介して張られるISP100とESP101との間の初期化用セッション確立ステップ600の処理の詳細を図8を参照して説明する。

【0053】(1) まず、初期化用セッションの確立の要求は、ISP100側から行われる。このため、ISP100は、FW102に対してコネクションを確立し、FW102に対してESP101との接続要求としてconnect.reqを発行する(ステップ800、801)。

【0054】(2) connect.reqを受けたFW102のメイン処理300は、接続先であるESP101とコネクション確立する。そして、メイン処理300は、ISP100へ接続完了応答connect.rspを返す(ステップ802、803)。

【0055】この接続完了応答connect.rspをISP100が受け取ることにより、FW102を介したISP100とESP101との間のセッションが確立される。前述の処理を終了したFW102は、以後データの中継だけを行う。前述した本発明の実施形態による処理は、FW102によるISP100の認証処理を行わず、ESP101がISP100の認証を行っている。

【0056】(3) 次に、ISP100は、trial.reqをESP101宛に送る。このtrial.reqには、乱数とその乱数をISP100及びESP101間の共通鍵で暗号化した値とが含まれており、これらがペアで送られる(ステップ804)。

【0057】(4) trial.reqを受けたESP101のメイン処理400は、送られた暗号化乱数を手持ちの共通鍵により解読し、解読した値が送られた乱数と一致したことによりISP100を確認する。そして、同様に乱数と暗号化した乱数とのペアをtrial.rspとしてISPメイン処理500に送る(ステップ805)。

【0058】(5) これを受けたISP100のメイン処理500は、先に述べたと同様の方法でESP101の認証を行う。次に、ISPメイン処理500は、初期化データをESP101へ送る(ステップ806)。

【0059】図9は前述した本発明の第1の実施形態におけるESPとISPとの間の初期化処理のロジックとFW処理のロジックとを説明するフローチャートである。9300はFWメイン処理300の処理フローであり、まず、これによりFW102の処理を説明する。

【0060】(1) FW102は、コネクションを中継

するタイプのFWである。このため、FW102は、まず、accept要求によりコネクションの受け付けを行い、次に、確立されたコネクションにより相手からの中継要求を受信する(ステップ9310、9320)。

(2) 次に、中継要求を送った相手の認証が必要か否かをチェックし、この結果、認証が必要であれば、認証処理を行う(ステップ9330、9340)。

(3) 次に、中継要求に記載された接続相手へのコネクションを要求を出し、中継先コネクションを確立する(ステップ9350)。

(4) 次に、ステップ9310で確立したコネクションとステップ9350で確立したコネクションとからのデータを相互に中継するため、これらコネクションを対応させる。そして、このようにして確立された中継路の確立完了応答を中継要求の送り主に対して返送する(ステップ9360)。

(5) そして、対応させたコネクション間でのデータの中継処理を行う(ステップ9370)。

【0061】9500はISPメイン処理500によるESP101とISP100との間の初期化処理ロジックの処理フローであり、以下、これについて説明する。

【0062】(1) まず、ISPメイン処理500は、FW102とのコネクションを確立し、FW102に対してESP101との中継要求を発行する(ステップ9510、9520)。

(2) 次にISPメイン処理500は、ESP101との間で認証を経ることにより登録を実行し、初期データをESP101へ送付する(ステップ9530、9540)。

【0063】9400はESPメイン処理400によるESP101とISP100との間の初期化処理ロジックの処理フローであり、以下、これについて説明する。

【0064】(1) まず、ESPメイン処理400は、FW102を介してISP100からのコネクションを受け付ける(ステップ9410)。

(2) 次に、ESPメイン処理400は、ISP101の認証を行い、当該ISP101を記憶し、ISP100からの初期データを受信する(ステップ9420、9430)。

【0065】図10は前述した本発明の実施形態におけるサーバ106とクライアント105上のそれぞれのアプリケーションプログラムの処理ロジックのフローチャートであり、図10を参照してクライアント用AP200とサーバ用AP2000との処理を説明する。

【0066】まず、クライアント用AP200の処理を説明する。

(1) まず、サーバ106と制御コネクションを確立し、次に、ユーザからのコマンドを受け付けて、転送要求か否かのチェックを行い、転送要求でなければ、当該コマンドの処理を行う(ステップ1010~103

0)。

(2) ユーザからのコマンドが転送要求であれば、サーバ106に制御コネクションによりデータ転送要求を通知し、自分の通信アドレスである通信ポートをTCP/IP処理203に依頼することにより、通信ポートを動的に割り当ててもらふ(ステップ1040、1050)。

(3) そして、割り当てられた通信ポートをサーバ106に通知し、サーバ106からの転送用コネクションを受け付ける(ステップ1060、1070)。

(4) 次に、ステップ1070の処理で確立した転送コネクションを用いてデータ転送を行う。その後、ステップ1020のユーザコマンドの受け付けの処理に戻る(ステップ1080)。

【0067】次に、サーバ用AP2000の処理フローを説明する。

(1) まず、クライアント105からのコネクションを受け付け、クライアントからの要求を受信する(ステップ2010、2020)。

(2) 次に、クライアントから受信した要求がデータ転送要求であるか否かを判別し、転送要求でなければ、要求に応じた処理を行う(ステップ2040、2030)。

(3) 受信した要求が転送要求であれば、クライアントAP200からのポート通知を受信するまで待つ(ステップ2050)。

(4) 次に、通知されたクライアントAP200のポート宛にコネクション要求を出すことにより転送コネクションを確立させ、確立した転送コネクションによりデータの転送を行う(ステップ2060、2070)。

【0068】図11は本発明の第1の実施形態におけるクライアント105上のソケットフック処理201の動作を説明するフローチャートであり、以下、これについて説明する。

【0069】(1) まず、ソケットフック処理201は、クライアント用AP200からの通信コマンドを受け取り、各コマンド毎に処理の振り分けを行う(ステップ1100)。

(2) 通信コマンドがconnectコマンドであった場合、まず、ESP101とコネクションを確立し、確立されたESP101とのコネクションを用いてFW102に対して、サーバ106への中継接続を要求する(ステップ1110、1112)。

(3) 次に、FW102による認証処理を行い、ESP101と暗号鍵を交換する(ステップ1114、1116)。

(4) 次に、ESP101を経由したFW102からの中継接続応答を受信し、リターンすることによりAPに応答を返す(ステップ1118、1160)。

【0070】(5) 通信コマンドがacceptコマン

ドであった場合、まず、ESP101からのコネクションを受け付けて、ESP101と鍵交換を行い、その後、リターンすることによりAPに応答を返す(ステップ1120、1122、1160)。

【0071】(6) 通信コマンドがsendコマンドであった場合、まず、データの暗号化を行い、ソケット処理202にコマンドを渡す。そして、ソケット処理202からのリターンをリターンすることによりAPに応答を返す(ステップ1130、1150、1160)。

【0072】(7) 通信コマンドがrecvコマンドであった場合、まず、ソケット処理202にコマンドを渡し、受信データの解読を行う。そして、リターンすることによりAPに応答を返す(ステップ1140、1142、1160)。

【0073】(8) 通信コマンドが前述以外のコマンドの場合、ソケット処理202にコマンドを渡し、ソケット処理202からのリターンをリターンすることによりAPに応答を返す(ステップ1150、1160)。

【0074】図12は本発明の実施形態におけるISPメイン処理300の処理を説明するフローチャートであり、以下、これについて説明する。

【0075】(1) まず、ISP100は、図9及び図8により説明したように、ESP101とのセッションを開設し、次に、ESP101からのコマンドを受信して、そのコマンドが接続要求(inside-connect.req)であるか否かを判断し、接続要求でなければ接続要求の受信待ちとなる(ステップ1200、1202)。

【0076】(2) ステップ1202で接続要求が受信されると、次に、サーバ106とのコネクションを確立し、次に、ESP101にサーバ106とのコネクションが確立したことを通知する(ステップ1204、1206)。

【0077】(3) 次に、データを受信し、中継処理を行う。このとき、サーバ106とのコネクションから受けたデータにISP-ESPプロトコルヘッダを付け、これをESPセッションでESP側へ転送する中継処理を行う(ステップ1208、1210)。

【0078】(4) 他方、ESPセッションから受信したデータは、そのデータ内容が判定される。それが通信アドレス通知でなければ、そのデータをサーバ106へ中継し、ステップ1208の処理に戻る(ステップ1212、1214)。

【0079】(5) ステップ1212で判定したデータ内容が通信アドレス通知であれば、ESP106宛に、クライアントとのコネクションを確立する要求を出し、次に、ESP106からのクライアントとのコネクションが確立したという確認応答を受信する(ステップ1216、1218)。

【0080】(6) 次に、データ内容の通信アドレスを

自分自信の通信アドレスに書き換えてデータの中継を行い、サーバからのコネクションを受け付けた後、ステップ1208の処理に戻る(ステップ1220、1222)。

【0081】図13は本発明の実施形態におけるESPメイン処理400の処理動作を説明するフローチャートであり、以下、これについて説明する。

【0082】(1) まず、ESP101は、図9及び図8により説明したように、ISP100とのセッションを開設し、次に、クライアント105からのコネクションを受け付けるまで待つ(ステップ1300、1302)。

【0083】(2) 次に、FW102とのコネクションを確立して、FW102への認証データの中継を行い、FW102からの応答を受信する。その後、FW102とのコネクションを切断する(1304～1310)。

【0084】(3) 次に、暗号鍵を生成してクライアントと交換し、サーバ106とのコネクションの要求をISP100に送る。そして、ISP100からのサーバ106とのコネクションが確立したことを示す応答メッセージを受信し、クライアント105へコネクション確立応答を送信する(ステップ1312～1318)。

【0085】(4) 次に、データの受信を行い内容で処理を振り分ける。そして、受信したデータが中継用のデータであれば、その受信データの中継を行って、データ受信のステップ1320に戻る。このとき、データのデータの暗号化・解読を行う(ステップ1320、1322)。

【0086】(5) ステップ1320で受信したデータがクライアントとのコネクション確立要求のデータであった場合、クライアント105とのコネクションを確立し、暗号鍵をクライアント105と交換する。そして、クライアント105とのコネクション確立応答をISP100に送信し、ステップ1320の処理に戻る(ステップ1324～1328)。

【0087】図14は本発明の第2の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0088】前述までに説明した本発明の第1の実施形態は、FW102を介してISP100とESP101との間で通信を行う例であったが、図14に示す本発明の第2の実施形態は、ISPとESPとの間を直接接続する通信路1400(例えば、LAN接続)を設け、通信路1400を用いてISPとESPとの間のセッションを確立し、初期化データや中継データを流すものである。

【0089】この本発明の第2の実施形態は、クライアント105のソケットフック処理201がFW102と接続するものとESP101と接続するものとを通信相手のアドレスにより振り分ける機能を持つ。このような

構成とすることにより、FW102の負荷を軽減することができるという効果を得ることができる。

【0090】図15は本発明の第3の実施形態によるネットワークシステムの構成例の一部を示すブロック図である。図15において、1500は計算機装置であり、他の符号は図1の場合と同一である。

【0091】前述した本発明の第1、第2の実施形態は、ISP100とESP101とを独立した計算機システムで実現した例であったが、図15に示す本発明の第3の実施形態は、1つの計算機装置1500内でISPメイン処理500とESPメイン処理400とを動作させるようにしたものである。そして、ISPメイン処理500とESPメイン処理400とは、FW102の内側と外側とのネットワークに接続されており、また、ISPメイン処理500とESPメイン処理400とは、プロセス間通信を行う。

【0092】前述のように、同一の計算機装置1500上にISPメイン処理500とESPメイン処理400とを実現することにより、動的通信アドレスを使用するAPをサポートするときの導入コストを抑えることができる。また、前述した本発明の第2の実施形態の場合と同様に、クライアント105のソケットフック処理201に、FW102と接続するものとESP101と接続するものとを通信相手のアドレスにより振り分ける機能を持たせることにより、FW102の負荷を軽減することができるという効果を得ることができる。

【0093】図16は本発明の第4の実施形態によるネットワークシステムの構成例の一部を示すブロック図であり、図の符号は図1の場合と同一である。

【0094】この本発明の第4の実施形態は、前述した本発明の第1の実施形態におけるFW102の上でISPメイン処理500とESPメイン処理400とFWメイン処理300とが動作するようにしたものである。そして、ISPメイン処理500とESPメイン処理400とFWメイン処理300とは、それぞれプロセス間通信を行うことによりデータの中継を実行する。

【0095】前述したように構成される本発明の第4の実施形態は、第3の実施形態よりも動的通信アドレスを使用するAPをサポートするときの導入コストを抑えることができる。

【0096】図17は本発明の第5の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0097】この本発明の第5の実施形態は、前述した本発明の第1の実施形態におけるサーバ106内に、デーモンプロセスとしてISPメイン処理500を実現するように構成したものであり、このような構成の実施形態においても、動的通信アドレスを使用するAPをサポートする場合の導入コストを抑えることができる。

【0098】図18は本発明の第6の実施形態によるネ

ットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0099】図18に示す本発明の第6の実施形態は、ESPをインターネット上のサーバとして実現したものであり、プロバイダISP100とESP101とを1対1のペアで存在させるのではなく、1つのESP101に対して複数のISP100がセッションを確立してデータの中継を行うことを可能にしたものである。

【0100】この実施形態によれば、ESP100を1つだけ設ければよいので、動的通信アドレスを使用するAPをサポートする場合の導入コストを抑えることができる。

【0101】図19は本発明の第7の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0102】図19に示す本発明の第7の実施形態は、前述した本発明の第1の実施形態におけるインターネットプロバイダ104内に、ESP101を1つの装置として実現したものである。そして、この実施形態においては、1つのISP100に対して複数のESP101がセッションを確立することができる。また、複数のISP100に対して複数のESP101が、多対多のセッションを確立することもできる。

【0103】前述のように構成される本発明の第7の実施形態によれば、サービスプロバイダのサービスとして動的通信アドレスを使用するAPをサポートしていることをアピールすることができる。

【0104】図20は本発明の第8の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0105】図20に示す本発明の第8の実施形態は、前述した本発明の第1の実施形態におけるクライアント計算機105上にESP101の機能を設けて構成したものであり、ESPメイン処理500を動作させソケットフック処理201で行うコネクション確立先アドレスをESPメイン処理500の内部アドレスにすることで容易に実現することができる。また、このとき、ESPとISPとの間のセッションの確立は、ESP101の側から起動をかけることにより行うことができる。

【0106】前述の本発明の第8の実施形態によっても、動的通信アドレスを使用するAPをサポートする場合の導入コストを抑えることができる。

【0107】図21は本発明の第9の実施形態によるネットワークシステムの構成例を示すブロック図であり、図の符号は図1の場合と同一である。

【0108】図21に示す本発明の第9の実施形態は、ISPメイン処理400をサーバ計算機106上に、ESPメイン処理をクライアント計算機105上に設け、さらに、パケットフィルタ機能をもつルータ103を備えて実現したものである。また、この実施形態におい

て、ESPとISPとの各機能をエンド計算機に持たせることも可能である。このとき、ISPとESPとの間の認証機能を利用することにより、FW102は認証機能を持つことが不要である。

【0109】前述の実施形態は、サーキットゲートウェイタイプのFWでなくパケットフィルタ型のFWにも適用することができる。

【0110】前述までに説明した本発明の各実施形態は、図6により説明したと同等な固定的なシーケンスしか実行することができないものであった。しかし、本発明は、より複雑な動的通信アドレスを使用したAPのサポートも行おうにすることができる。いか、その例を説明する。

【0111】図22はISP100が入力するAP個別対応のアクセス制御マクロ言語の一例を示す図である。

【0112】図22において、initial service-addressは、サーバアプリケーションのよく知られた通信サービスアドレスが記述される。ISP partは、ISP100におけるデータ内容のチェック条件と条件が一致したときの処理とをISP-ESPプロトコルを含めてマクロ記述したものである。また、ESP partも同様である。

【0113】ISP100は、前述のようなマクロに合わせてAPデータ解析処理501やESPプロトコル処理502を拡張する機能と、ESP101に対する初期化データを生成する機能を持つ。ESP101は、ISP100から送られたデータに基づいてISPプロトコル処理403を拡張する機能を持つ。なお、ISP100が、ESP101で実行可能なオブジェクトを送付して、ESP101がこれを実行するような形態をとってもよい。

【0114】前述により、より複雑な動的通信アドレスを使用したAPのサポートを容易に行うことが可能になる。また、複数のESP101を接続するISP100は、それぞれのESP101におけるアクセス制御ポリシーを別個に指定することができ、その設定を一括して行うことができるため、拡張性を含めて運用管理しやすいものとすることができる。

【0115】前述した本発明の各実施形態は、ISP100がデータをチェックするとして説明したが、本発明は、ESP101側でデータチェックするようにすることも容易に実現できる。また、この実現においては、図22で説明したように、ユーザがそのチェック条件を指定するようにすればよい。これにより、不要なデータをISP101が受け取ることがないため、安全性を高めることができ、かつ、ISP100の負荷も軽減することができる。

【0116】図23は本発明の第10の実施形態によるネットワークシステムの構成例を示すブロック図である。

【0117】前述までに説明した本発明の各実施形態は、ESP101をインターネット111の側に接続した例であったが、図23に示す本発明の第10の実施形態は、ESP101を他のイントラネット110bに設けて構成したものである。すなわち、図23に示す実施形態は、2つのイントラネット110a、110bを設け、一方のイントラネット110bの側にESP101を設けたものである。

【0118】図23に示す実施形態は、前述の構成を備えることにより、他のイントラネット内のクライアント105と自イントラネット内のサーバ106との間で通信を行うことができ、サーバを異なるイントラネットに移動させても通信を行うことができるという効果を得ることができる。

【0119】

【発明の効果】以上説明したように本発明によれば、以下に説明するような効果を得ることができる。

【0120】1. 既存のFWを使用したネットワーク環境で、動的通信ポートを使用するAPを、そのAPを改造することなく使用して、FWを介した安全な通信を行うことが可能となる。

【0121】2. また、FWが暗号をサポートしている環境で、動的通信ポートを使用するAPを、そのAPを改造することなく適応させることができる。

【0122】3. 同様に、FWで認証機能をサポートした環境で、動的通信ポートを使用するAPを、そのAPを改造することなく適応させることができる。

【0123】4. また、FWで暗号をサポートしない環境で、動的通信ポートを使用するAPを、APを改造することなく適応させることができ、かつ、暗号化をサポートすることも可能となる。

【0124】5. さらに、既存のFWを使用したネットワーク環境で、動的通信ポートを使用する複数のAPを、それらのAPを改造することなくサポートしたとき、各APのアクセス制御情報を纏めて作成し、各装置に反映させることができるため管理や運用を行いやすい。

【0125】6. また、前記5のアクセス制御情報の反映時、反映するデータが暗号化されているため、管理や運用のセキュリティを確保することができる。

【0126】7. また、本発明は、認証機能をサポートしているので、確実な相手とのみデータ転送を行うことができセキュリティを高めることができる。

【0127】8. また、FWを仲介しないデータ転送路を確保した本発明は、FWの負荷を軽減しネットワーク性能の向上を図ることができる。

【0128】9. また、異なるイントラネットを介して特定のAPを使用して通信を行うことができる。

【0129】10. また、自社製業務用APを使用してインターネットからFWで区切られた自社イントラネッ

ト内のサーバと通信するとき、自社製のAP用のAPGWを作成する必要がなく、その構築コストを抑えることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図2】図1におけるクライアント計算機のソフトウェア構成を説明する図である。

【図3】図1におけるFWのソフトウェア構成を説明する図である。

【図4】図1におけるESPのソフトウェア構成を説明する図である。

【図5】図1におけるISPのソフトウェア構成を説明する図である。

【図6】本発明の第1の実施形態によるネットワークシステムにおけるESPとISPとの間のプロトコルを説明するシーケンス図である。

【図7】図6により説明したISPとESPとの間の通信プロトコルメッセージのフォーマットを説明する図である。

【図8】ISPとESPとの間の初期化用セッション確立の処理を説明するシーケンス図である。

【図9】前述した本発明の第1の実施形態におけるESPとISPとの間の初期化処理のロジックとFW処理のロジックとを説明するフローチャートである。

【図10】前述した本発明の実施形態におけるサーバとクライアント上のそれぞれのアプリケーションプログラムの処理ロジックのフローチャートである。

【図11】本発明の第1の実施形態におけるクライアント上のソケットフック処理201の動作を説明するフローチャートである。

【図12】本発明の実施形態におけるISPメイン処理300の処理を説明するフローチャートである。

【図13】本発明の実施形態におけるESPメイン処理400の処理動作を説明するフローチャートである。

【図14】本発明の第2の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図15】本発明の第3の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図16】本発明の第4の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図17】本発明の第5の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図18】本発明の第6の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図19】本発明の第7の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図20】本発明の第8の実施形態によるネットワークシステムの構成例を示すブロック図である。

【図21】本発明の第2の実施形態によるネットワークシステムの構成例を示すブロック図である。

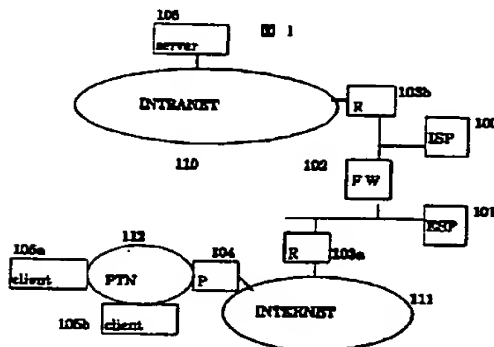
【図22】ISP100が入力するAP個別対応のアクセス制御マクロ言語の一例を示す図である。

【図23】本発明の第10の実施形態によるネットワークシステムの構成例を示すブロック図である。

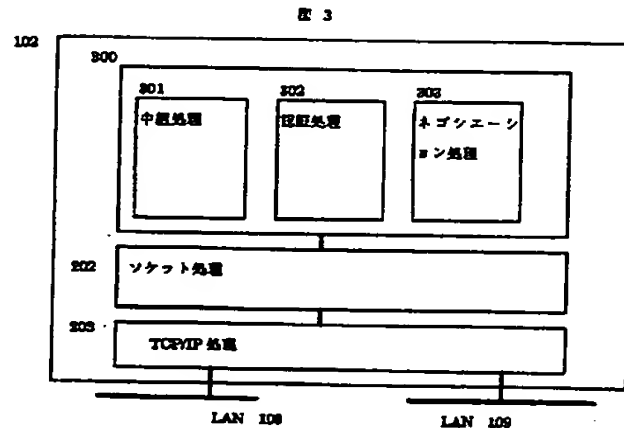
【符号の説明】

- 100 内部セキュリティ代行サーバ (ISP)
- 101 外部セキュリティ代行サーバ (ESP)
- 102 ファイアウォール (FW)
- 103 ルータ (R)
- 104 インターネットプロバイダ (P)
- 105 クライアント計算機
- 106 サーバ計算機
- 110 イントラネット
- 111 インターネット
- 112 公衆電話網 (PTN)

【図1】

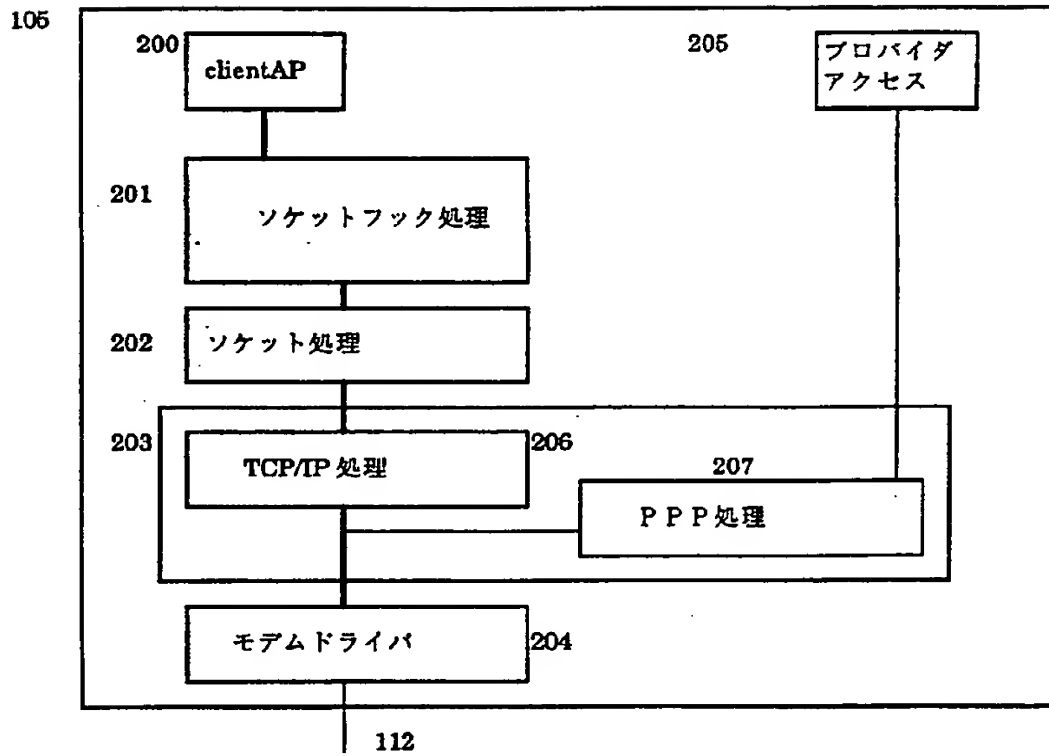


【図3】



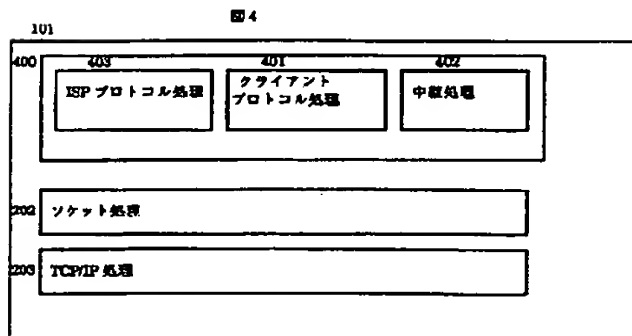
【図 2】

図 2



【図 4】

【図 5】



【図 15】

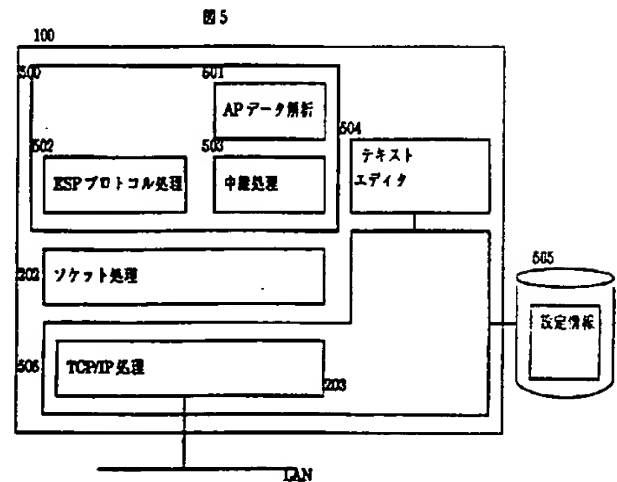
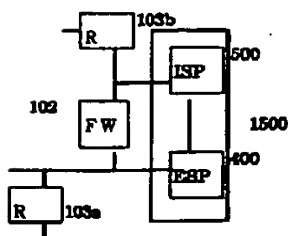
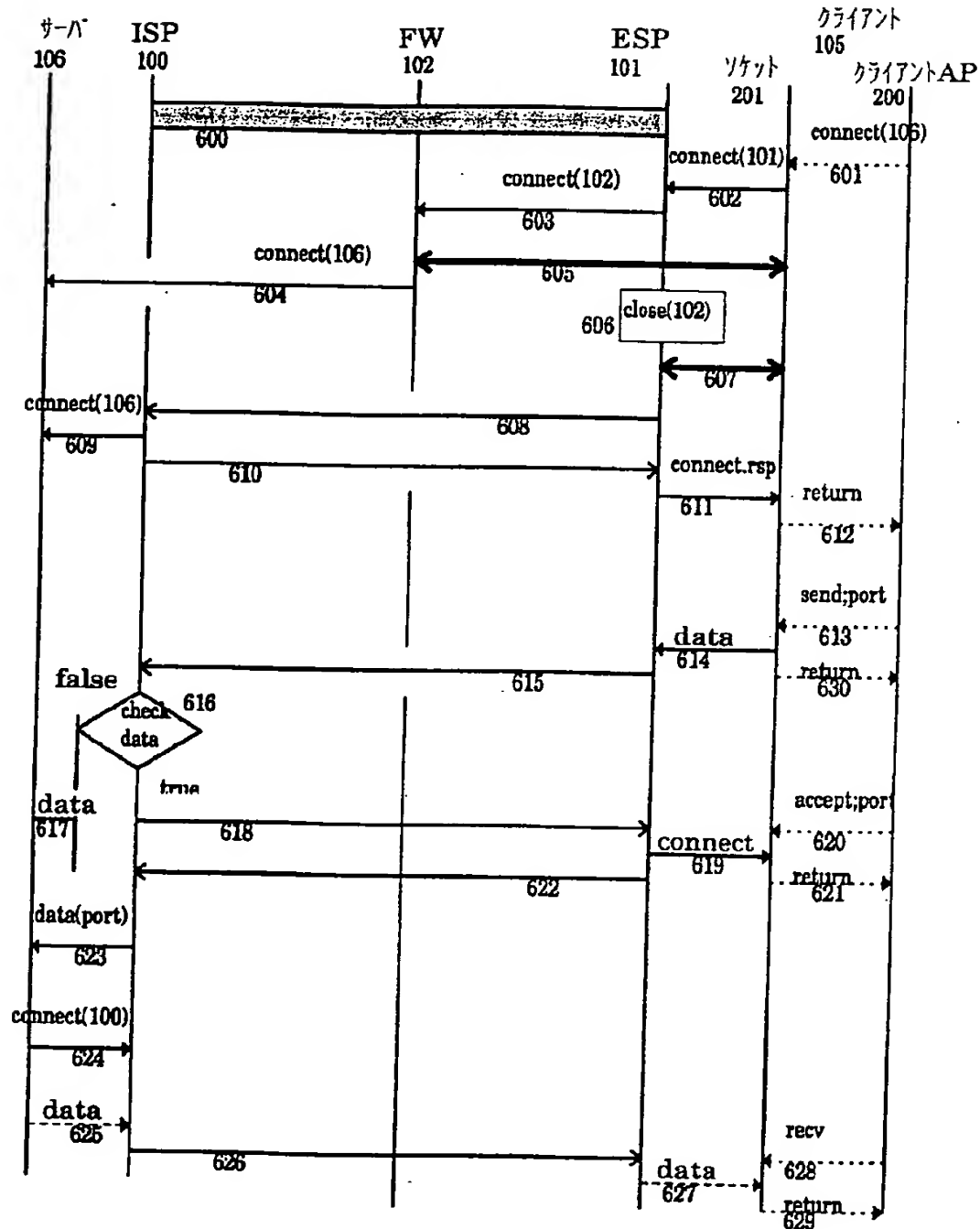


図 15

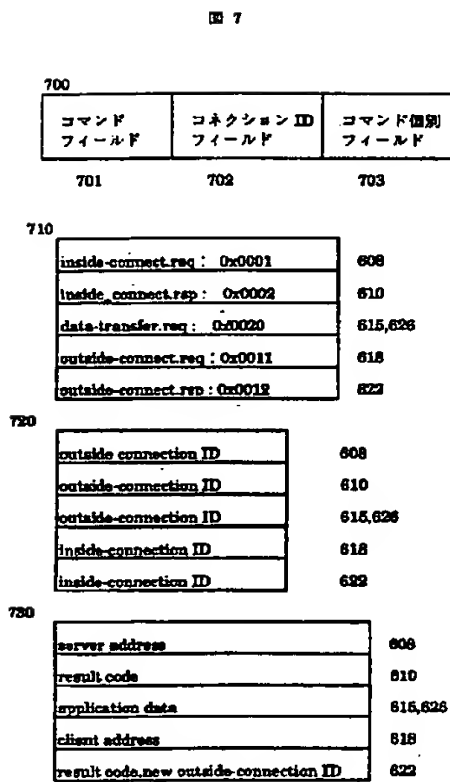


【図6】

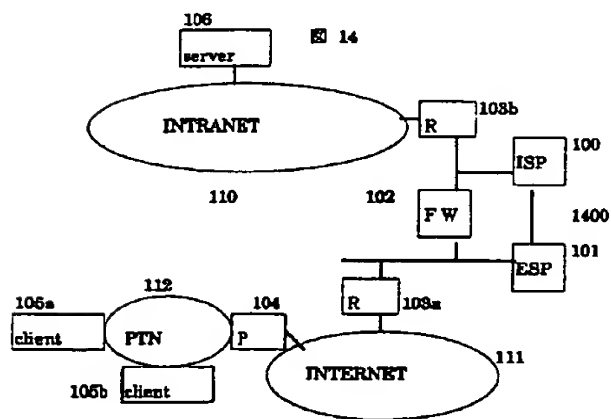
図 6



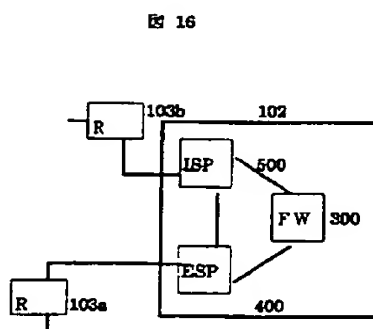
【図 7】



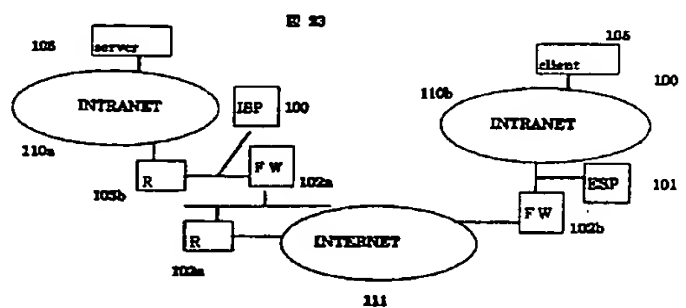
【図 14】



【図 16】

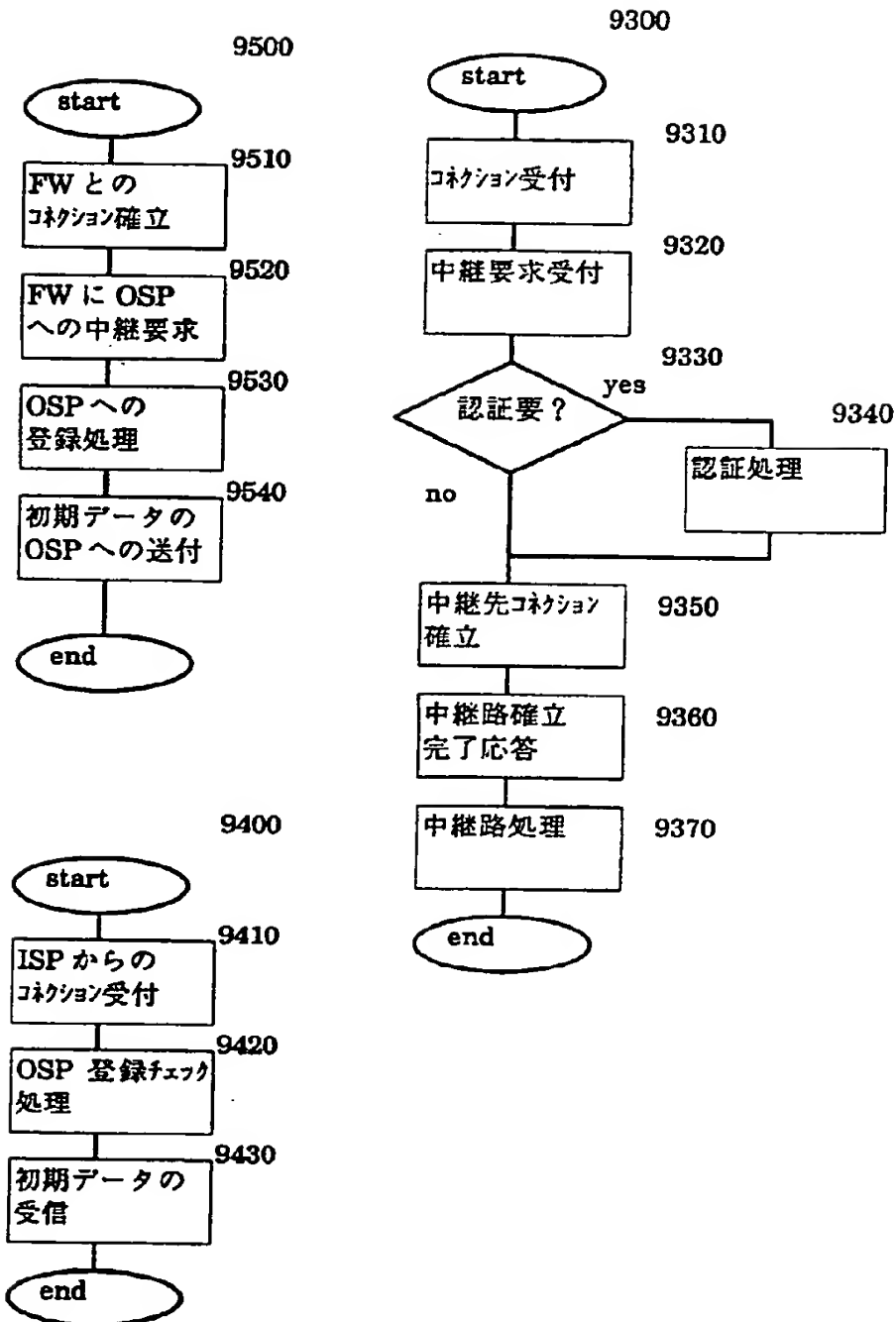


【図 23】



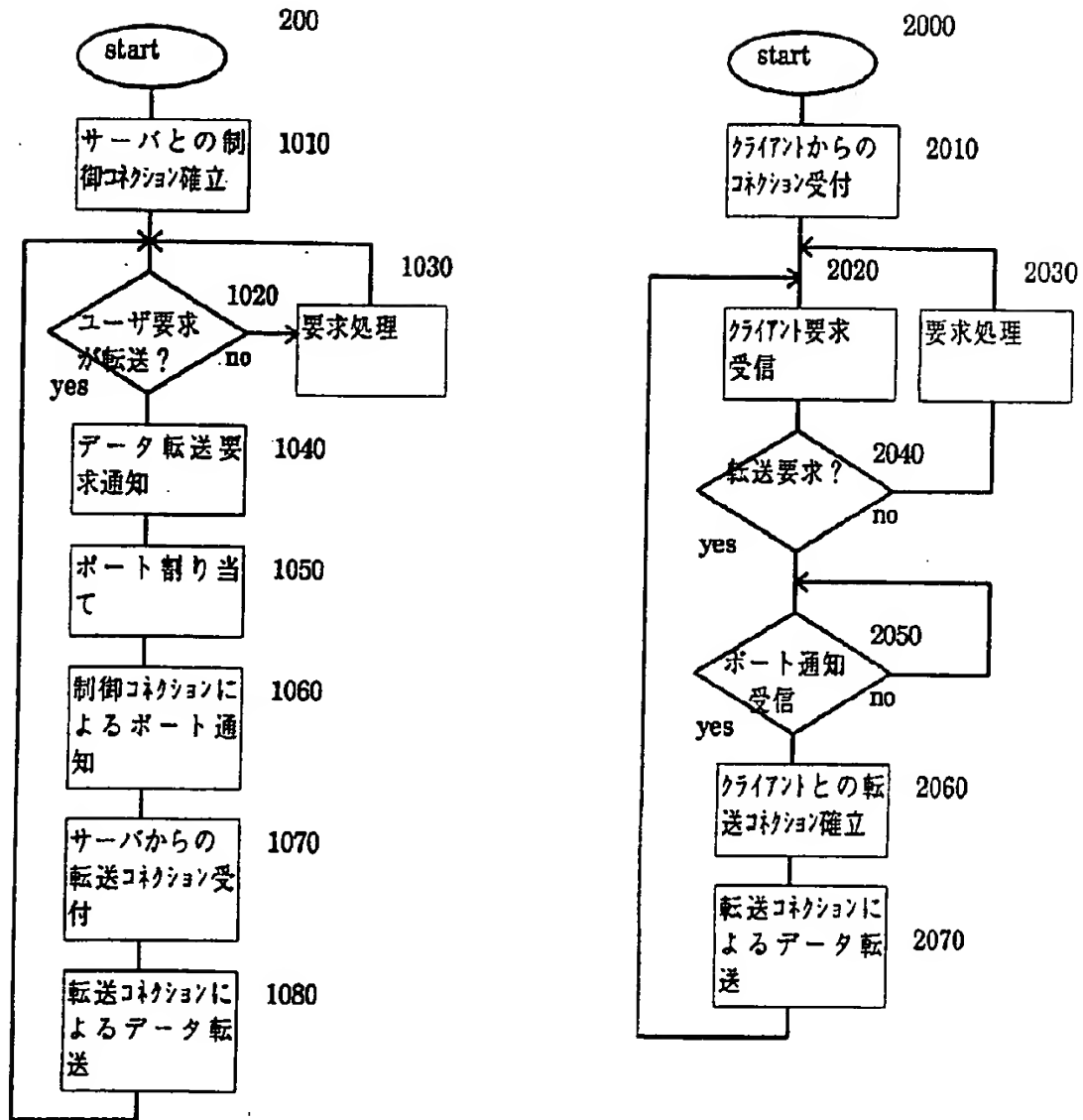
【図9】

図 9



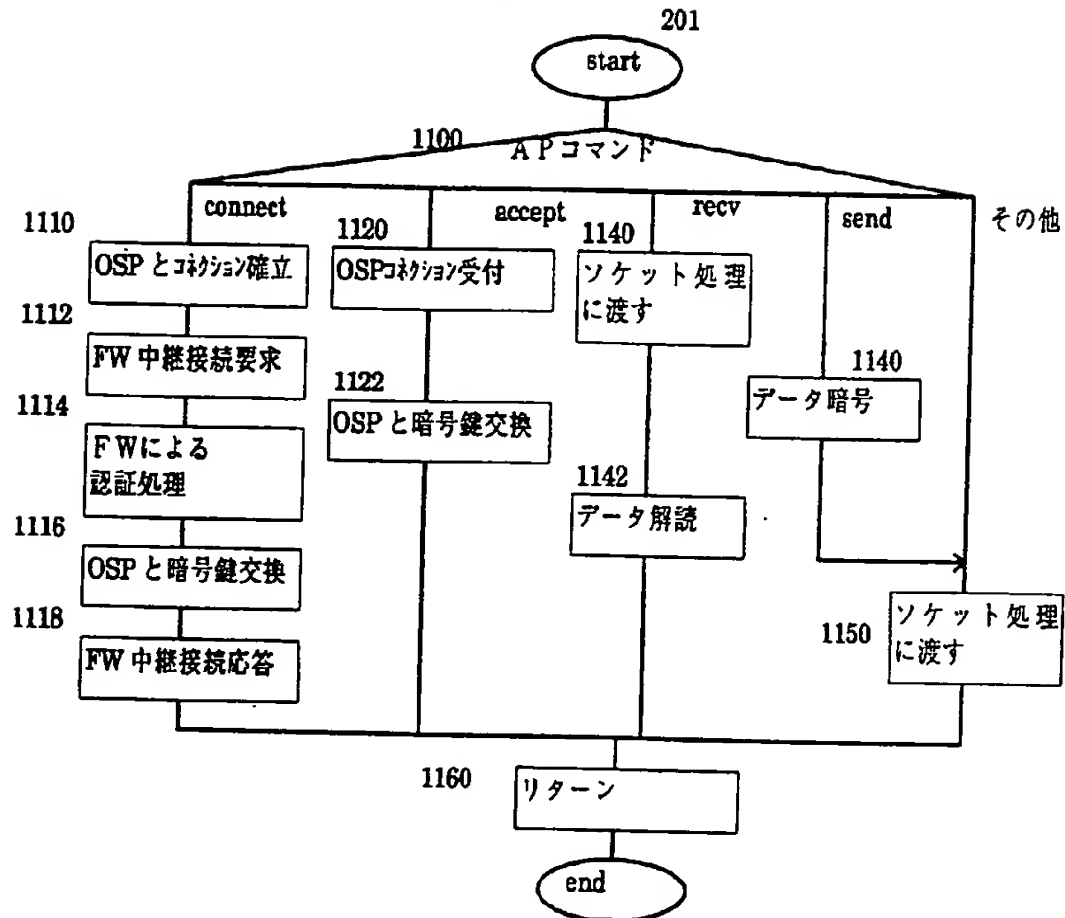
【図10】

図10

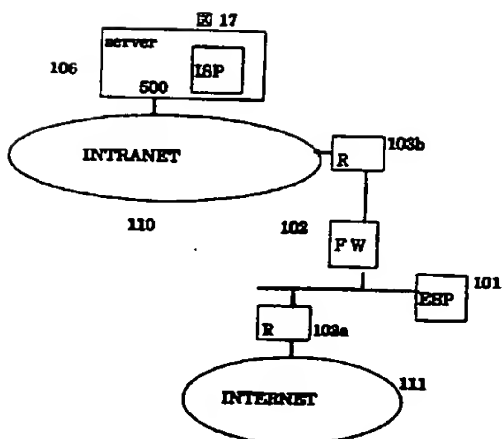


【図 11】

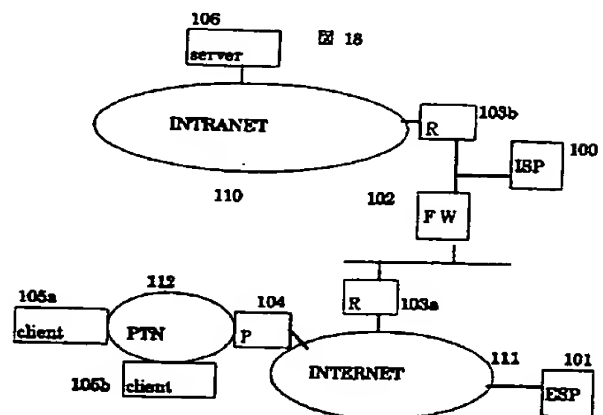
図 11



【図 17】



【図 18】



【図 12】

【図 22】

図 12

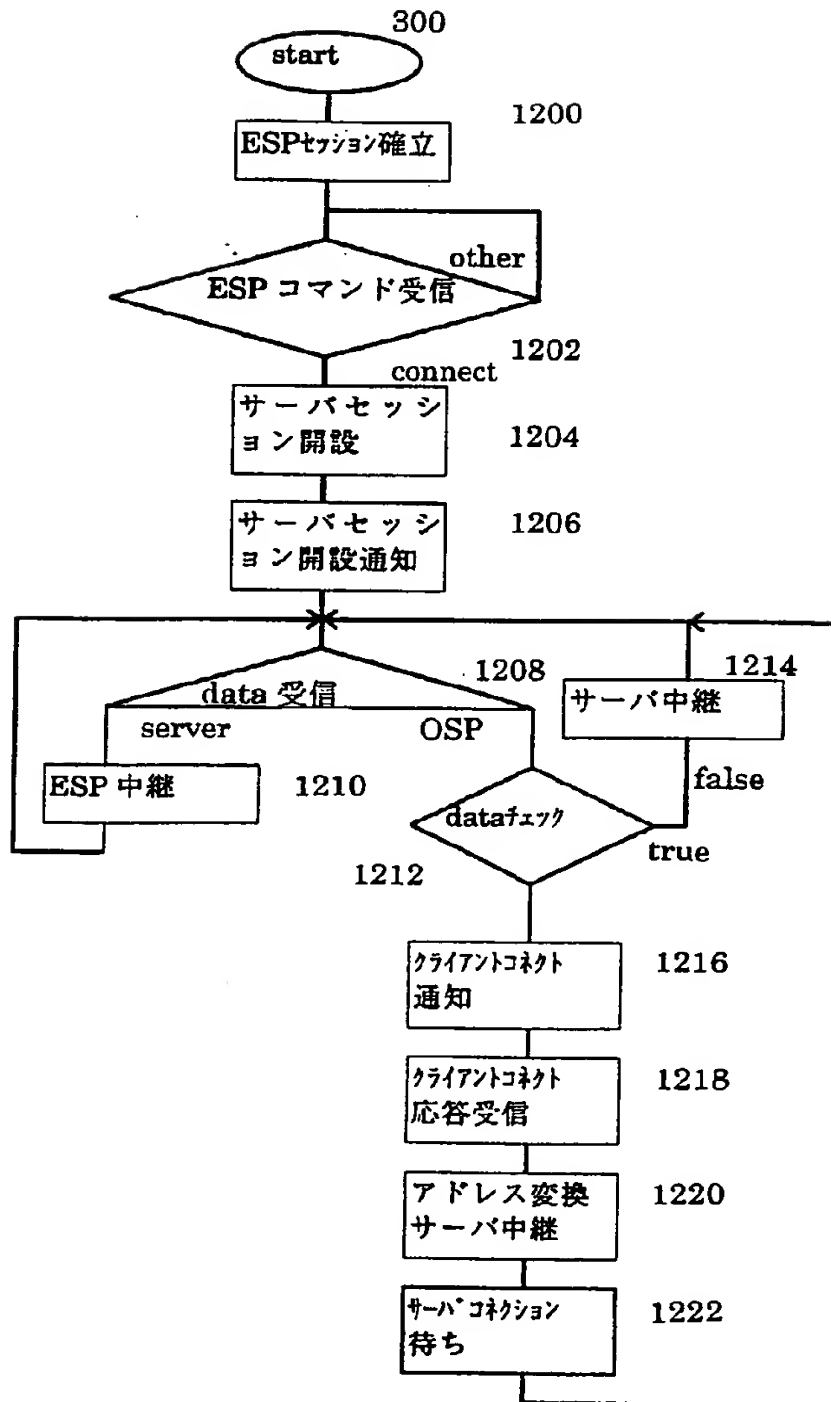


図 22

```

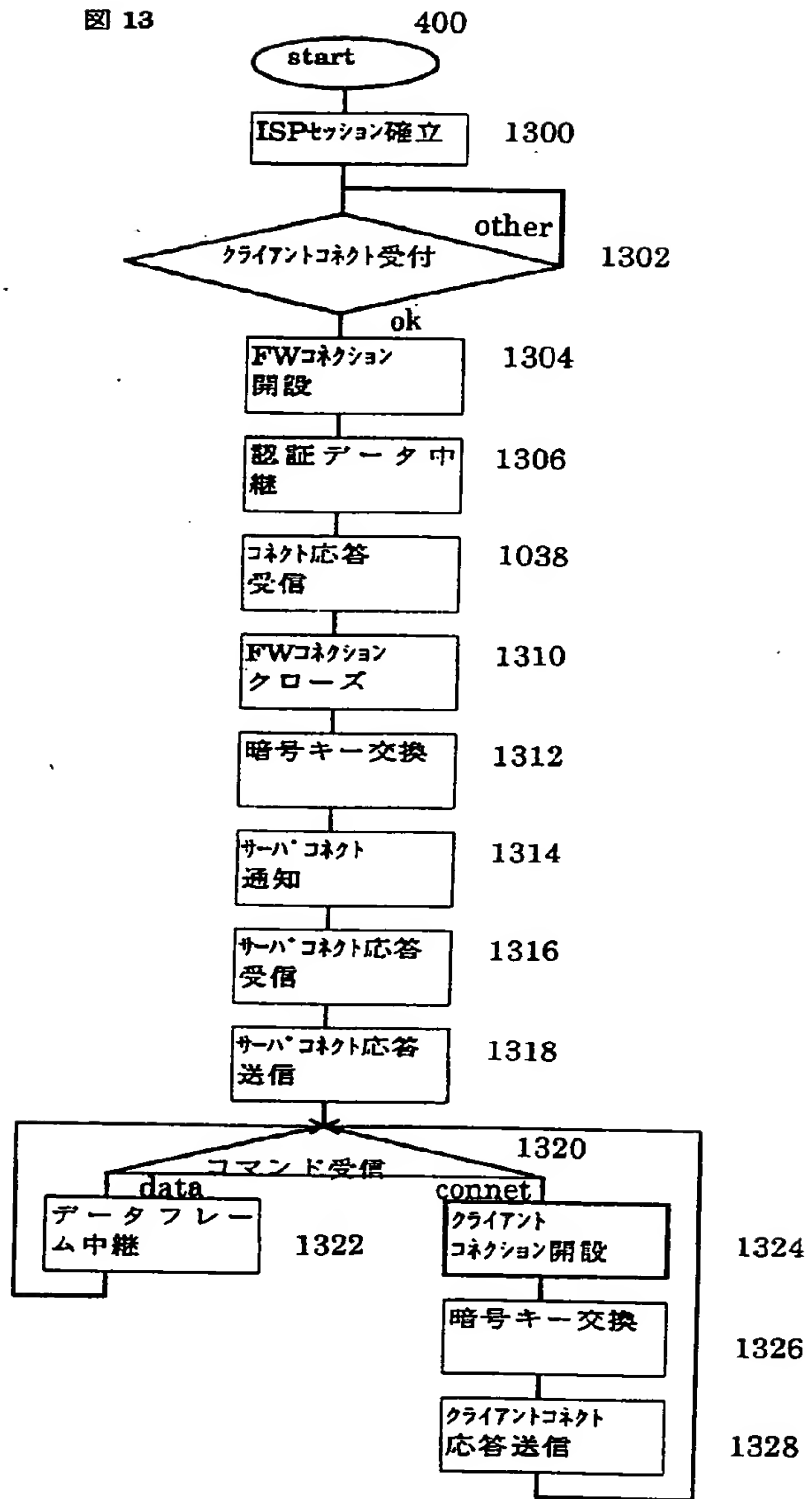
# AP ACCESS CONTROL MACRO
initial service-address = xxx.xxx.xxx.yyy.yyy
ISP part
{
  if (Top_Data == "PORT")
  {
    Change_address;
    Accept;
    Send p1;
    if (Recv p2) { Forward_L; }
  }
}

ESP part
{
  if (Recv p1)
  {
    Connect;
    Key_Change;
    Send p2;
    Forward_E;
  }
}

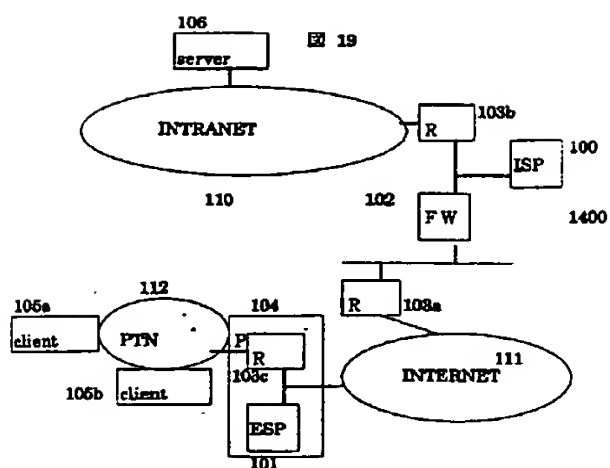
```

【図13】

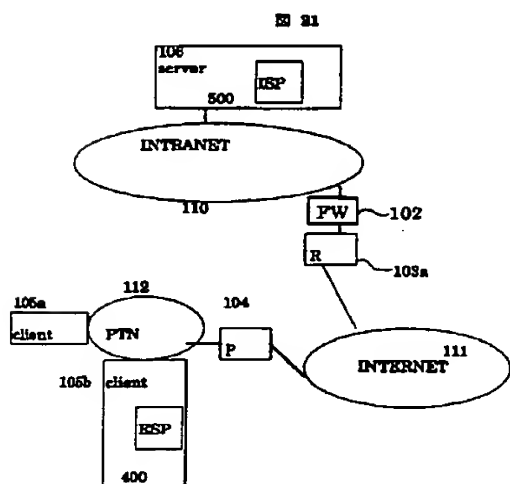
図 13



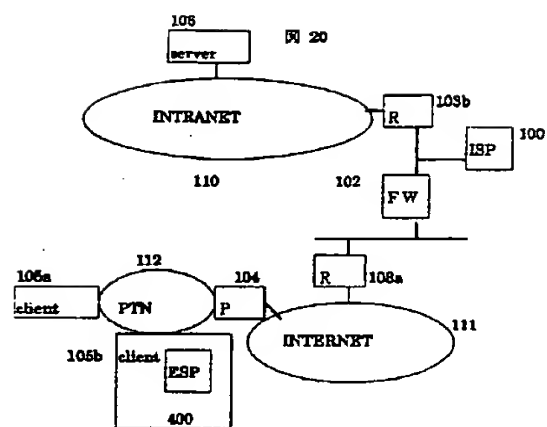
【図 19】



【図 21】



【図 20】



フロントページの続き

(51) Int. Cl. 6

識別記号

F I

H O 4 L 12/24

12/26

THIS PAGE BLANK (USPTO)